Configurare i criteri di Windows in AMP for Endpoints

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Modalità e motori](#)
[Esclusioni](#)
[Proxy](#)
[Controllo delle epidemie](#)
[Aggiornamenti prodotti](#)
[Impostazioni avanzate](#)
[Salva modifiche](#)
[Informazioni correlate](#)

Introduzione

In questo documento vengono descritti i componenti configurabili nei criteri di Windows di Advanced Malware Protection (AMP) for Endpoints.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Utente AMP for Endpoints con privilegi di amministratore

Componenti usati

Le informazioni fornite in questo documento si basano su AMP for Endpoints Console.

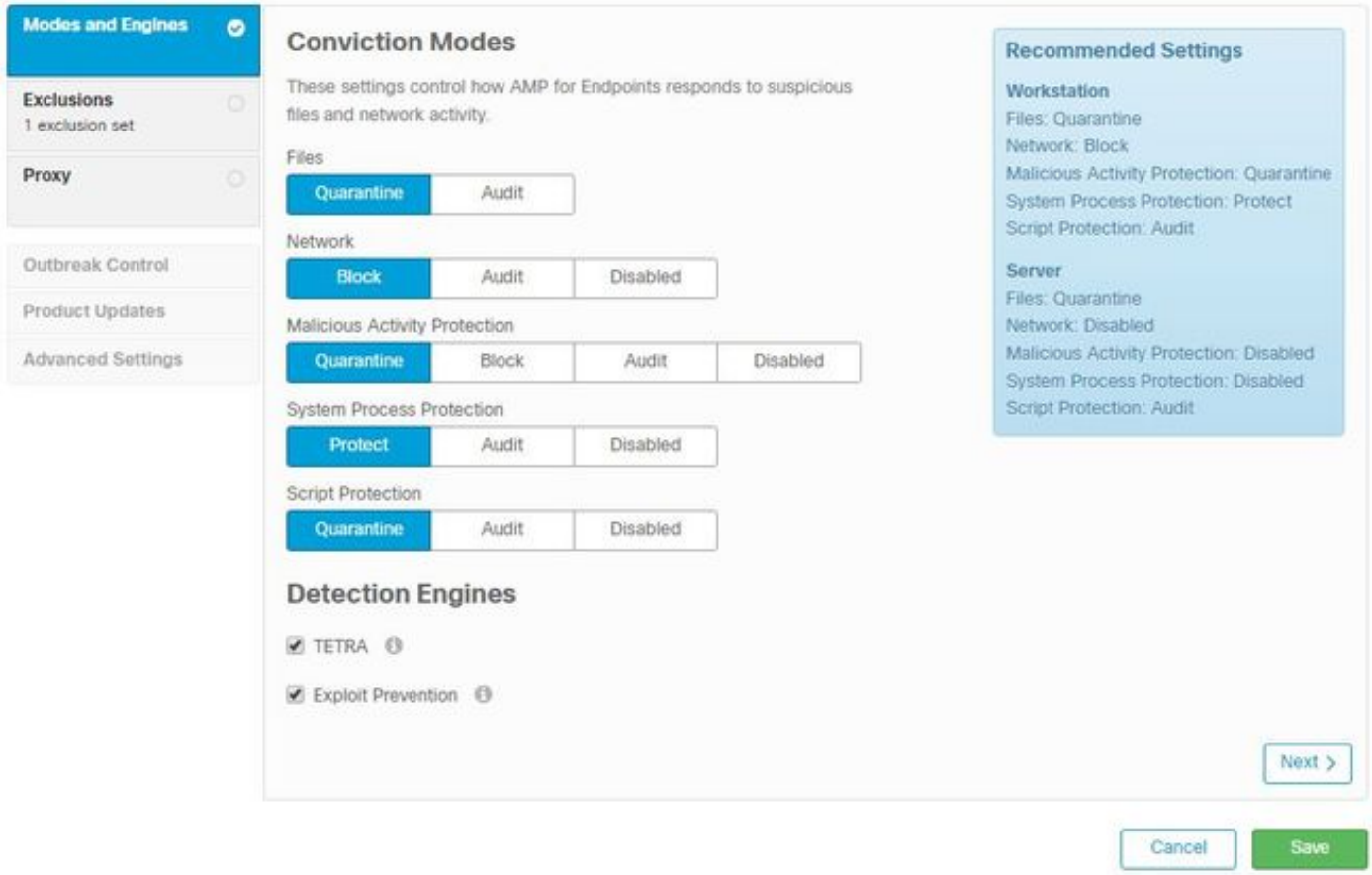
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Per creare un nuovo criterio di Windows, passare alla scheda Gestione e selezionare Criteri. Nella

sezione dei criteri creare un nuovo criterio di Windows.

Modalità e motori



File: Il motore SHA principale e la funzionalità di base di AMP. Questa opzione consente l'analisi dei file e la messa in quarantena.

Rete: Il motore Device Flow Correlation per il monitoraggio delle connessioni.

Protezione da attività dannose: Motore che protegge l'endpoint dagli attacchi ransomware.

Protezione dei processi di sistema: Motore che protegge i processi di sistema critici di Windows dai compromessi attraverso attacchi di aggiunta di memoria.

Protezione script: Fornisce visibilità sugli attacchi basati su script.

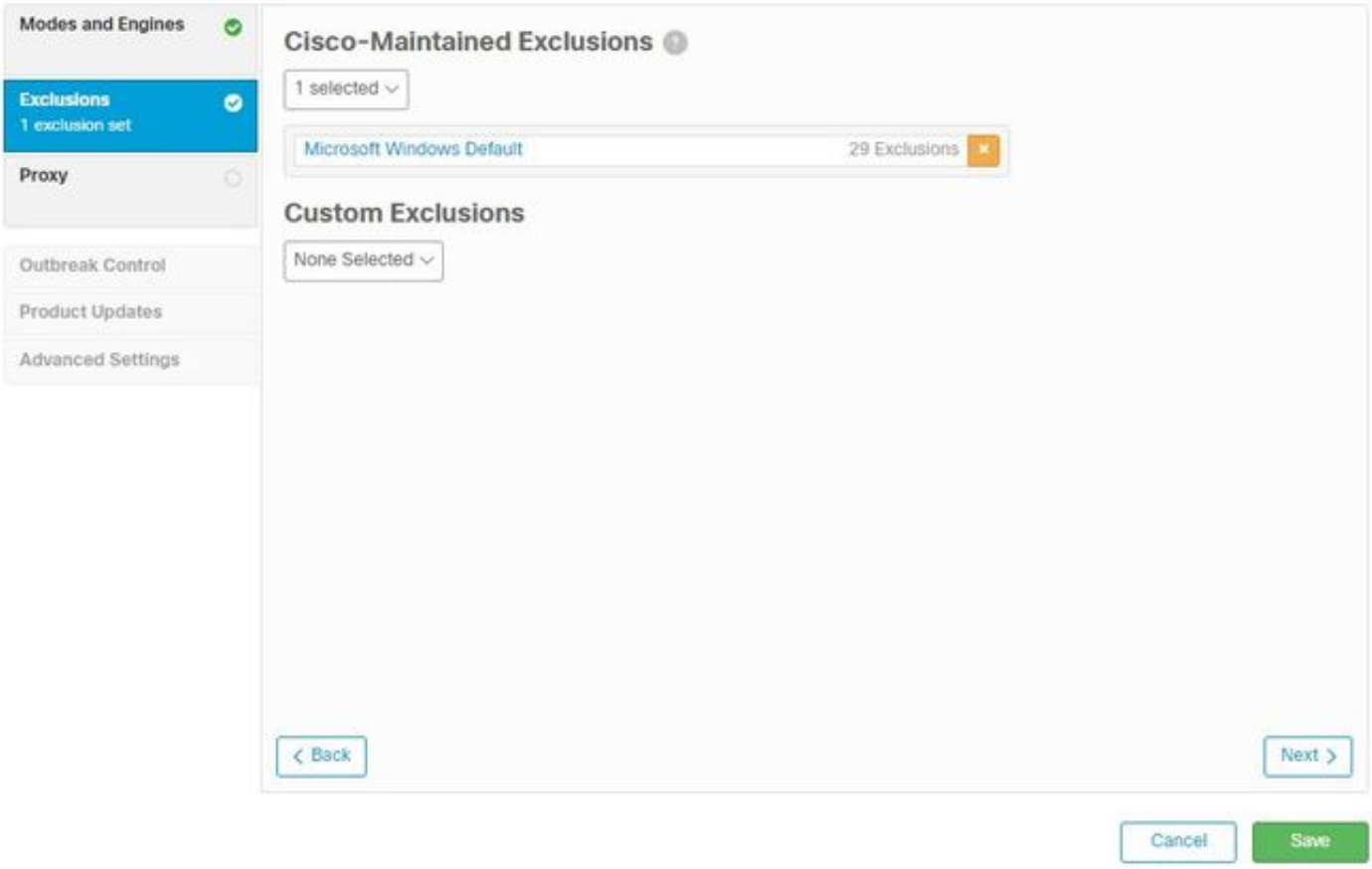
Motori di rilevamento:

- Tetra: Antivirus offline che scarica le definizioni per proteggere l'endpoint
- Prevenzione degli attacchi: Protegge i connettori dagli attacchi di inserimento della memoria

Nota: Nella sezione a destra viene visualizzata una finestra delle impostazioni consigliate per Workstation e Server.

Dopo aver configurato la sezione Modi e motore, fare clic su **Avanti**, come mostrato nell'immagine.

Esclusioni



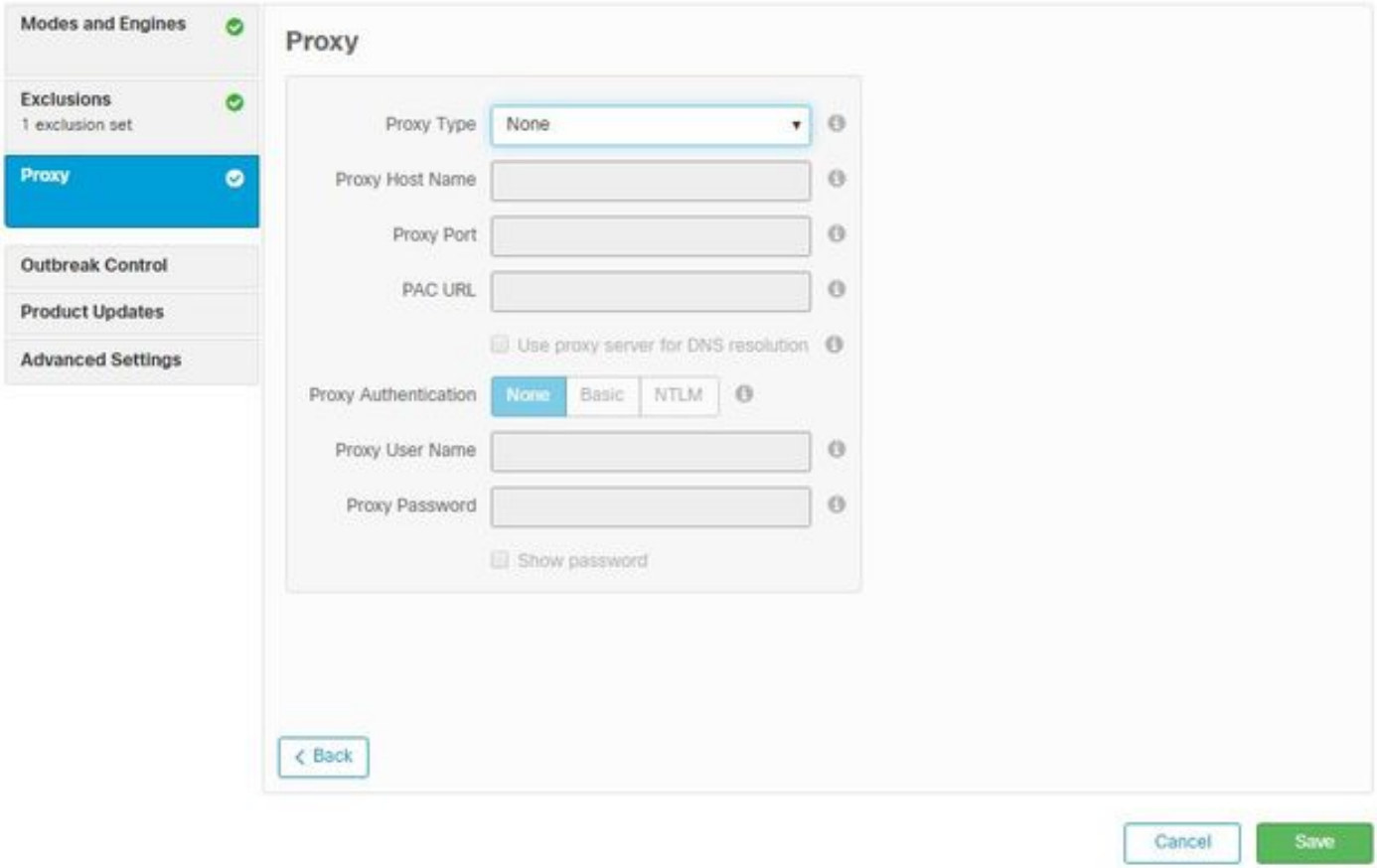
La sezione delle esclusioni contiene Esclusioni gestite da Cisco ed esclusioni personalizzate:

- Le esclusioni gestite da Cisco sono create e gestite da Cisco e consentono di escludere le applicazioni comuni dalle scansioni eseguite da AMP per evitare problemi di incompatibilità
- Le esclusioni personalizzate vengono create e gestite dall'amministratore utente

Per ulteriori informazioni sulle esclusioni, vedere questo video.

Al termine della configurazione delle esclusioni, fare clic su **Avanti**, come mostrato nell'immagine.

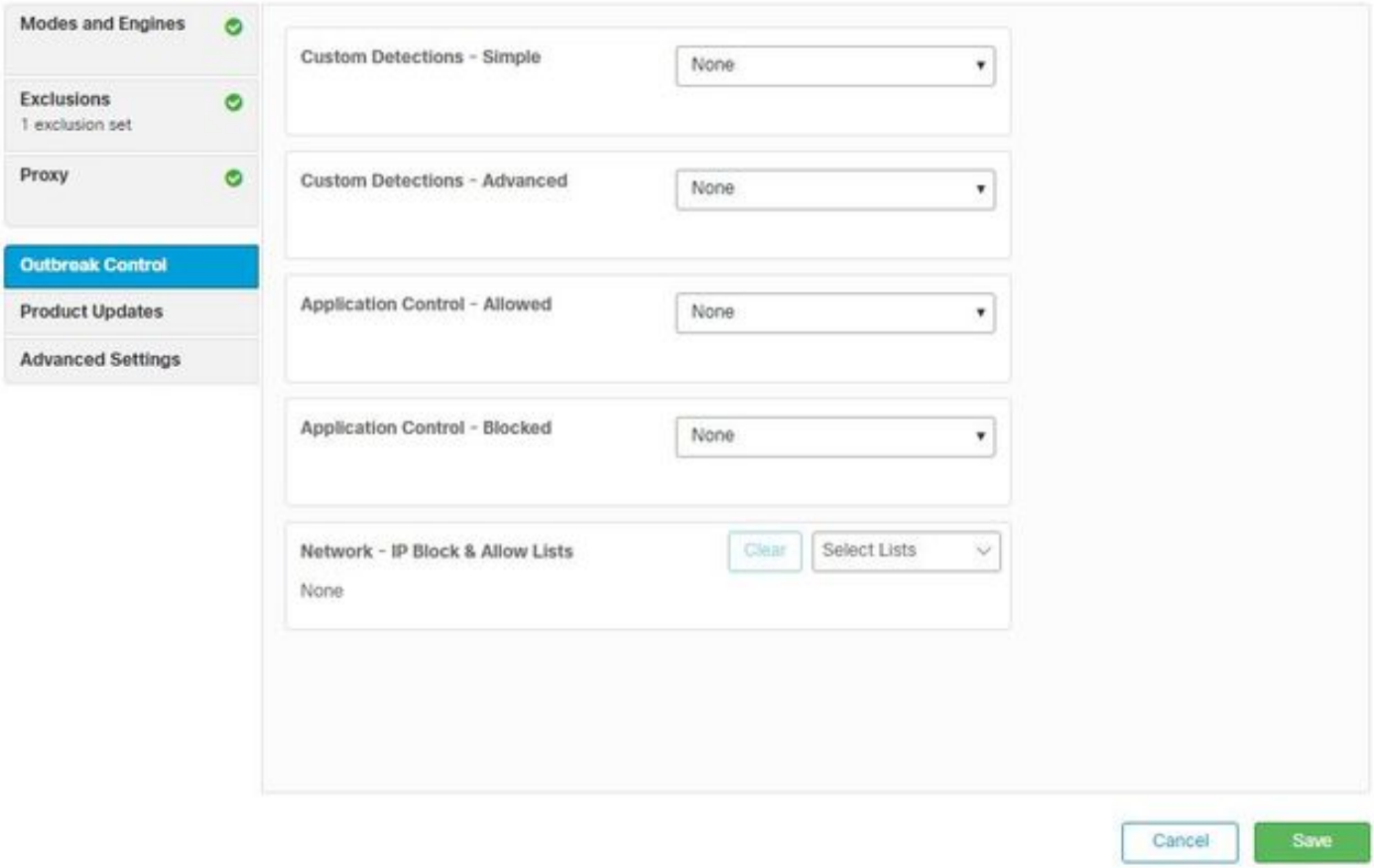
Proxy



In questa sezione è possibile configurare le impostazioni proxy per l'ambiente in uso per consentire al connettore di eseguire query sul cloud AMP.

Dopo aver configurato le impostazioni del proxy, fare clic su **Salva**, come mostrato nell'immagine.

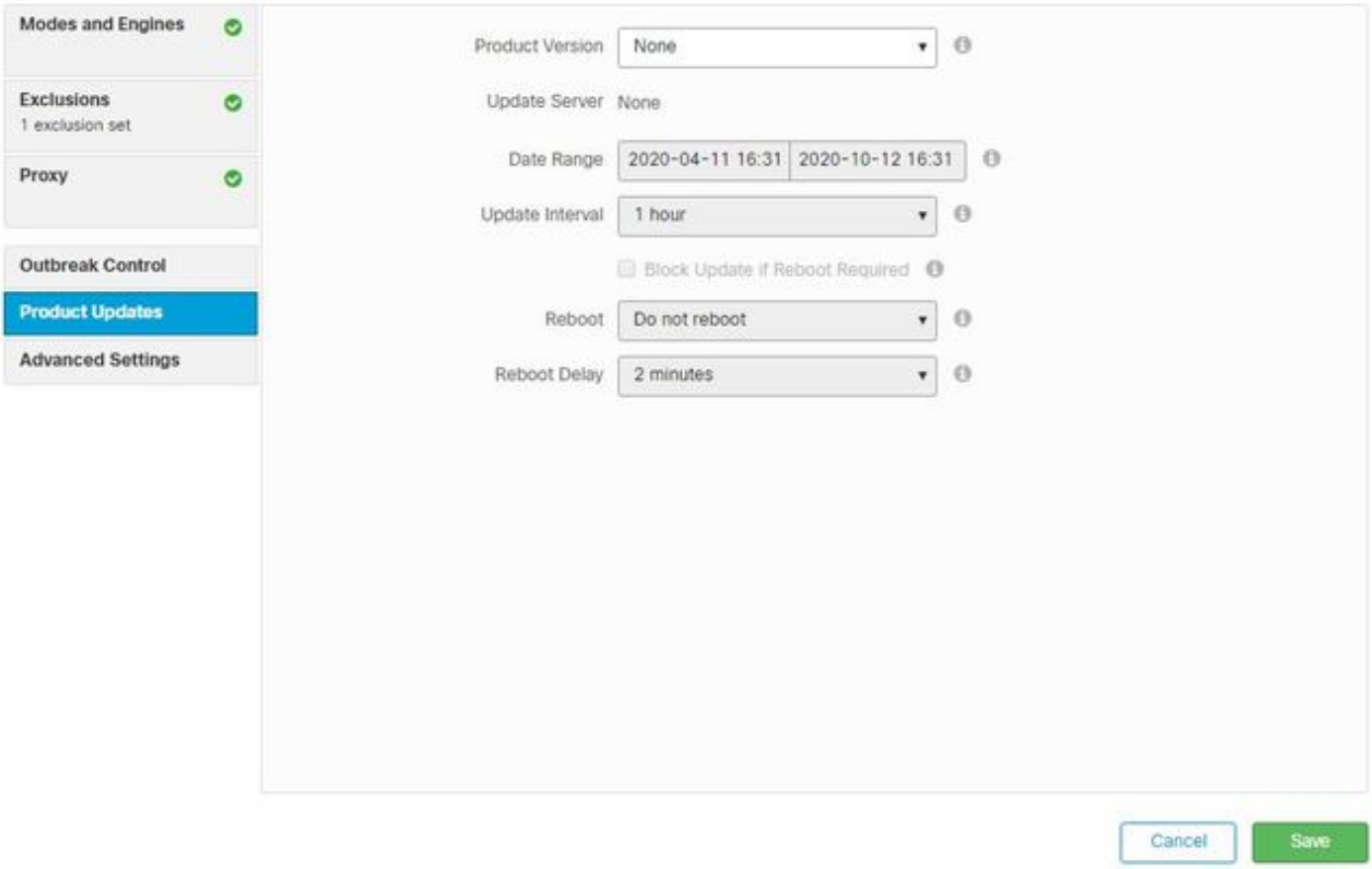
Controllo delle epidemie



Nella sezione Controllo epidemie è possibile configurare rilevamenti personalizzati:

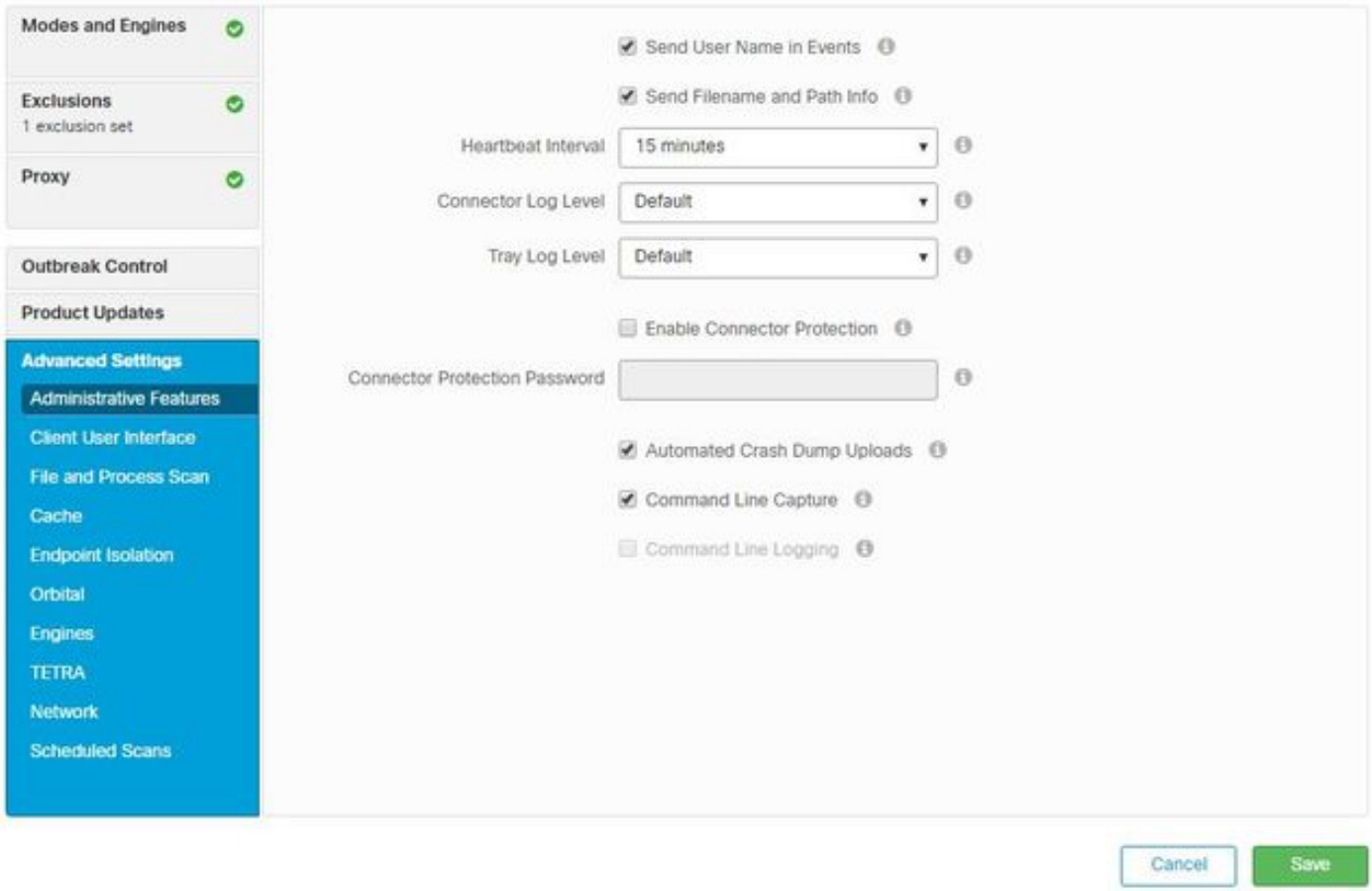
- Rilevamenti personalizzati - Semplice: Consente di bloccare file specifici in base al relativo SHA
- Rilevamenti personalizzati - Avanzati: Blocca i file in base alle firme per i rilevamenti quando un'istanza di Agente integrità sistema semplice non è sufficiente
- Elenchi applicazioni consentite e bloccate: Consente o blocca le applicazioni con Agenti integrità sistema
- Rete - Elenchi indirizzi IP bloccati e consentiti: utilizzata con Device Flow Correlation (DFC) per definire rilevamenti di indirizzi IP personalizzati

Aggiornamenti prodotti



Nella sezione Product Update sono impostate le opzioni per i nuovi aggiornamenti. È possibile scegliere una versione, un intervallo di date per eseguire il rollover degli aggiornamenti e le opzioni per il riavvio.

Impostazioni avanzate



Funzioni amministrative: Configura la frequenza con cui il connettore interroga il cloud per le modifiche al criterio.

Interfaccia utente client: Consente di controllare la visualizzazione delle notifiche nei dispositivi in cui è installato AMP.

Analisi di file e processi: configura le opzioni di protezione in tempo reale, il modo in cui i connettori controllano le disposizioni dei file e le dimensioni massime consentite per i file.

Cache Configurazione di Time To Live per la cache.

L'isolamento degli endpoint consente di attivare e configurare la funzionalità per isolare i dispositivi con il connettore AMP installato.

L'opzione Orbital attiva la ricerca orbitale avanzata.

Motori: Impostazioni per ETHOS; un motore di raggruppamento file e SPERO; un sistema di apprendimento automatico.

Configurazione TETRA per il motore offline.

Rete Abilita le opzioni di Correlazione flusso dispositivo.

Nella sezione Scansioni pianificate è possibile configurare le opzioni relative al momento e al tipo di analisi da eseguire nei connettori.

Salva modifiche

Dopo aver apportato le modifiche desiderate, fare clic su **Salva** per assicurarsi che vengano applicate al criterio.

Le informazioni contenute in questo documento sono inoltre disponibili nel video Configurazione dei criteri di Windows in AMP for Endpoints.

Informazioni correlate

- Per ulteriori informazioni sulla configurazione dei criteri, consultare la Guida dell'utente
- **Documentazione e supporto tecnico – Cisco Systems**